The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/13/2010

SUBJECT:
Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (MS10-081)

OVERVIEW:
A vulnerability has been discovered in the Windows Common Control Library that could allow an attacker to take complete control of a vulnerable system. The Windows Common Control Library is a set of interfaces that enables a user to interact with an application and is used by all supported versions of the Windows Operating System. Many popular third-party programs utilize this interface including web browsers such as Mozilla Firefox and Google Chrome.

This vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
Windows XP
Windows Vista
Windows Server 2003
Windows Server 2008
Windows 7

RISK:
Government:
Large and medium government entities:**High**
Small government entities:**High**

Businesses:
Large and medium business entities:**High**
Small business entities:**High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in the Windows Common Control Library that could allow an attacker to take complete control of a vulnerable system. The Windows Common Control Library is a set of windows that enables a user to interact with an application. The common control library, Comctl32.dll, is included as part of all supported versions of the Windows Operating System.

Scalable Vector Graphics (SVG) is a series of specifications of an XML-based file format for describing two-dimensional graphics. SVG is an open standard, proposed by the World Wide Web Consortium (W3C). Numerous third-party programs provide support for SVG, including browsers such as Mozilla Firefox, Google Chrome, Opera and web browser plug-ins such as SVG Web.

The Windows Common Control Library incorrectly handles certain messages when processing scalable vector graphics (SVG) passed from a third-party SVG viewer. This vulnerability may be exploited if a user visits or is

redirected to a specifically crafted web page. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights.

It should be noted that a system with a default Windows configuration is not vulnerable to this issue. Microsoft Internet Explorer does not contain native support for SVG. The system must have a third-party SVG viewer installed in order to be vulnerable.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the appropriate patch provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-081.mspx

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2746

SecurityFocus:
http://www.securityfocus.com/bid/43717